

VERWERKERSOVEREENKOMST T.B.V. Raamovereenkomst Adviesdiensten Energiesystemen

Tussen

De gemeente Arnhem / Verwerkingsverantwoordelijke



En

Naamopdrachtnemer / Verwerker

Logo

Geel: = <invulveld> of keuze

Referentienummer Gemeente Arnhem: 4460049

Datum:

Ondergetekenden

Gemeente Arnhem, waarvan <het college van Burgemeester en Wethouders/de Gemeenteraad> de verwerkingsverantwoordelijke is, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie> daartoe bevoegd op grond van het 'Algemeen ondermandaat-, ondervolmacht- en ondermachtigingsbesluit....zaaknummer

en

<Bedrijf>, gevestigd te <plaatsnaam>, KVK-nummer <nummer> verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam>, <functie>,

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwegen het volgende:

- a) Partijen hebben op <datum> de <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: <specificatie dienst(en)>;
- b) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
- c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
- d) Partijen willen in aanvulling op de UAVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

Artikel 1 Definities

- 1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
- 1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

Artikel 2 Ingangsdatum en duur

- 2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.
- 2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.
- 2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

- 3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
- 3.2 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.

Artikel 4 Inhoudelijke afspraken

- 4.1 **Beveiligingsmaatregelen**
Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. De wijze waarop Verwerker de passende technische en organisatorische maatregelen aantoont, staat in Bijlage 2.
- 4.2 **Audits**
Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.
- 4.3 **Verwerking buiten de EER**
Verwerker verwerkt persoonsgegevens in beginsel enkel binnen de EER. Verwerker mag Persoonsgegevens buiten de Europese Economische Ruimte (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan vooraf op de hoogte.
- 4.4 **Geheimhouding**
Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.

4.5 Subverwerkers

De ten tijde van het afsluiten van deze Verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1. Verwerkingsverantwoordelijke verleent hierbij algemene toestemming voor de inschakeling van subverwerkers. Verwerker houdt voor de start van de werkzaamheden Verwerkingsverantwoordelijke op de hoogte van de beoogde inschakeling van nieuwe subverwerkers. Bij de inschakeling van subverwerkers blijven artikel 28.2 en 28.4 AVG onverkort van kracht.

4.6 Rechten van betrokkenen

Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Verwerker Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.

4.7 Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging

Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

Artikel 5 Inbreuk in verband met Persoonsgegevens

- 5.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.
- 5.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen.
- 5.3 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.
- 5.4 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 6 Aansprakelijkheid

- 6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.

Artikel 7 Beëindigen verwerkersovereenkomst

- 7.1 Partijen moeten in de Hoofdovereenkomst afspraken maken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens.
- 7.2 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 8 Overige bepalingen

- 8.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Hoofdovereenkomst.

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <.....>

Gemeente Arnhem

<Naam organisatie>

namens deze: <naam, functie>

namens deze: <naam, functie>

plaats: <.....>

plaats: <.....>

datum: <.....>

datum: <.....>

Bijlage 1: Overzicht van te verwerken persoonsgegevens

Met opmerkingen [TS1]: In de vullen door de opdrachtgever samen met de verwerker (leverancier)

1. Naam verwerking, doeleinden categorieën van betrokkenen, categorieën persoonsgegevens en eventuele doorgifte naar derde landen.

Naam verwerking	Verwerkingsdoeleinden	Categorieën van Betrokkenen	Categorieën Persoonsgegevens (waaronder bijzondere persoonsgegevens)	Verwerkingslocatie	Doorgifte-instrument (indien van toepassing)	Aanvullende maatregelen (indien van toepassing)
<i>Beschrijf hier de opdracht</i>	<i>Beschrijf hier het doel van de opdracht</i>	<i>Voorbeelden van categorieën van betrokkenen :</i> <i>Aanvragers/Indieners</i> <i>Belanghebbers</i> <i>Bestuurders/Raadsleden</i> <i>Collegeleden</i> <i>Ambtenaren gemeente</i> <i>Websitebezoekers</i> <i>Personeel leveranciers</i> <i>Ouderen</i> <i>Gehandicapten</i> <i>Kinderen</i> <i>Inwoners van ..</i>	<i>Voorbeelden van persoonsgegevens:</i> <i>Personeelsgegevens (denk aan salaris, ziekte, rechtspositie etc)</i> <i>NAW gegevens (+telefoonnummers, emailadressen en postcode /huisnummers)</i> <i>CV</i> <i>Sollicitatiebrieven</i> <i>Videomateriaal , audiomateriaal</i> <i>Identificatienr., paspoortnr., BTW nummer ZZP-er</i> <i>Gebruikersnaam, wachtwoord</i> <i>BSN</i> <i>IP-adres, online surfgedrag,</i>	<i>Als persoonsgegevens worden doorgegeven naar (of toegankelijk zijn in) een land buiten de EER moet dat hier worden aangegeven . Stem dit af met PO.</i>		

Met opmerkingen [TS2]: De verwerker dient aan te geven welk doorgifte-instrument wordt er gebruikt. De doorgifte-instrumenten zijn:

1. Adequaatheidsbesluit
2. Specifieke uitzonderingen (art. 49).
3. Standaard bepalingen (standard contractual clauses SCCs);
4. Bindende bedrijfsvoorschriften (binding corporate rules, BCRs);
5. Gedragsregels (codes of conduct; -certificationmechanisms);
6. Ad hoc modelcontractbepalingen (ad hoc contractual clauses).

Met opmerkingen [TS3]: Volgens de aanbevelingen van de EDPB n.a.v. de Schrems II uitspraak van het Hof van Justitie van de EU (Recommendations 01/2020, d.d. 10 november 2020) moeten aanvullende maatregelen genomen worden als gebruik wordt gemaakt van doorgifte-instrument 3 – 6. Zo wordt nl. een aan de AVG gelijkwaardig beschermingsniveau bewerkstelligd (zie Bijlage 2 van de EDPB aanbevelingen).

Met opmaak: Regelaafstand: Meerdere 1,15 rg

			<p><i>cookies</i></p> <p><i>Locatiegegevens</i></p> <p><i>Naam, geboortedatum, geboorteplaats, geslacht, gezinssamenstelling</i></p> <p>Voorbeelden van bijzondere gegevens:</p> <p><i>Biometrische gegevens met het oog op de unieke identificatie van een persoon</i></p> <p><i>Financiële gegevens</i></p> <p><i>Genetische gegevens</i></p> <p><i>Gezondheidsgegevens</i></p> <p><i>Lidmaatschap van een vakbond</i></p> <p><i>Politieke opvattingen</i></p> <p><i>Ras of etnische afkomst</i></p> <p><i>Religieuze of levensbeschouwelijke overtuigingen</i></p> <p><i>Seksueel gedrag of seksuele gerichtheid</i></p> <p><i>Strafrechtelijke</i></p>		
--	--	--	---	--	--

			<i>persoonsgegevens</i>			
--	--	--	-------------------------	--	--	--

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke voor het melden van datalekken (NB: Ook buiten kantooruren)	Mail naar privacy@arnhem.nl indien er sprake is van: <ul style="list-style-type: none"> • Een datalek • Wijziging van (sub) verwerker(s) • Vragen inzake deze verwerkersovereenkomst
Contactpersoon Verwerker (NB: Ook buiten kantooruren)	Naam: Contactgegevens: <input type="text"/>
Contactgegevens IBD	Telefoonnummer 070-204 55 11 e-mailadres: privacy@vng.nl

Met opmerkingen [TS4]: In te vullen door de verwerker (leverancier)

NB: Eventuele wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

3. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen	Toepassing (geautomatiseerd systeem)	Verwerkingslocatie	Doorgifte instrument (indien van toepassing)	Aanvullende maatregelen (indien van toepassing)

Met opmerkingen [TS5]: In te vullen door de verwerker (leverancier).

Een subverwerker is een partij die namens de verwerker persoonsgegevens verwerkt voor de verantwoordelijke. Dit is vaak het geval wanneer verwerkers andere partijen inschakelen voor de uitvoering van de verwerking.

Bijlage 2: Aantonen passend niveau van beveiliging

Normenstelsel

☐ De verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten:

..... (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, ISO 27001, PCI/DSS) en is volgens deze norm **wel/niet** gecertificeerd.

☐ De verwerker werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, te weten:

☐ De verwerker werkt volgens een andere norm, te weten:

NB: Het is voor de verwerker verplicht te beschikken over informatiebeveiligingsbeleid waarin, of waarnaast, opgenomen is welke beheersmaatregelen getroffen zijn ten behoeve van:

- de interne organisatie
- de veiligheid van personeel
- het beheer van bedrijfsmiddelen en informatieclassificatie
- fysieke beveiliging
- acquisitie, ontwikkeling en onderhoud van informatiesystemen
- leveranciersrelaties
- beheer van informatiebeveiligingsincidenten

Al deze beheersmaatregelen zijn direct te herleiden uit algemeen erkende overheidsnorm BIO.

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- ☐ Certificering;
- ☐ Verklaring van toepasselijkheid (VVT);
- Rapportages van periodieke externe controles zoals:
 - ☐ Audits,
 - ☐ Pentesten of
 - ☐ TPM's (bijv. ISAE3xxx SOC type II);
 - ☐ Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
 - ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO, een ICV):

NB: Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1. **NB.** Ook al betreft het een eigen controle of eigen mededeling: onafhankelijkheid ten behoeve van deze mededeling dient altijd aantoonbaar en geborgd te zijn.

Met opmerkingen [TS6]: In te vullen door de verwerker (leverancier). Aanvinken en aanvullen welke norm van toepassing is. En laten beoordelen door de ISO/CISO.

Met opmerkingen [TS7]: Wanneer je een systeem aanschaft waarbinnen veel gevoelige data wordt verwerkt dient de verwerker zowel een pentest als een TPM aan te leveren.

Met opmerkingen [TS8]: In te vullen door de verwerker (leverancier). Aanvinken waaruit de toereikendheid van de informatiebeveiliging blijkt. De verwerker dient de aangevinkte informatie aan te leveren. Stuur dit bewijs door naar de CISO/ISO ter beoordeling.

Wanneer het aangeleverde bewijs van toereikendheid is goedgekeurd door de CISO/ISO laat je deze informatie door de contractmanager opnemen in het inkoopdossier.

Versie 2.5.1



Aansluiting bij goedgekeurde gedragscode

- ☐ Verwerker is aangesloten bij een door een toezichhoudende autoriteit goedgekeurde gedragscode, te weten

Bijlage 3: Inlichtingen om Inbreuken te beoordelen

Verwerker zal alle inlichtingen verschaffen die de Verwerkingsverantwoordelijke noodzakelijk acht om het Incident of Inbreuk te kunnen beoordelen. Daarbij verschaft Verwerker in ieder geval de volgende informatie aan de Verwerkingsverantwoordelijke:

- (Vermeende) oorzaak van de inbreuk;
- (Vooralsnog bekende en/of te verwachten) gevolg van de inbreuk;
- (Voorgestelde) oplossing voor de gevolgen van de inbreuk en van nieuwe inbreuken;
- Contactgegevens van de verantwoordelijke manager;
- Aantal betrokkenen (exact of geschat of basis van minimale en maximale aantallen);
- Korte omschrijving van de Betrokkenen;
- Het soort of de soorten Persoonsgegevens waarop de inbreuk is gepleegd;
- Datum waarop inbreuk heeft plaatsgevonden (indien geen exacte datum: periode waarbinnen inbreuk heeft plaatsgevonden);
- Datum en tijdstip, waarop de inbreuk bekend is geworden bij Verwerker of bij een door hem ingeschakelde derde of onderaannemer;
- Of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden, inclusief eventuele andere toegepaste maatregelen;
- De reeds ondernomen maatregelen om de (nieuwe) inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken;
- De te nemen maatregelen om in de toekomst dergelijke Incidenten of Datalekken te voorkomen/beperken.